AF
IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Alan Dowd et al.

Title: NETWORK SECURITY MODELING SYSTEM AND METHOD

Docket No.: 105.176US1
Filed: January 14, 2000
Examiner: Dwin M. Craig

Serial No.: 09/483,127
Due Date: January 14, 2005
Group Art Unit: 2123

Mail Stop Appeal Brief--Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

We are transmitting herewith the following attached items (as indicated with an "X"):

X Appellants' Brief On Appeal Under 37 CFR 41.37(c) (26 pgs.), including authorization to charge Deposit Account 19-0743 in the amount of $250.00 to cover the Appeal Brief Filing Fee.

X Petition for Extension of Time (1 pg.), including authorization to charge Deposit Account 19-0743 in the amount of $1080.00 to cover the Extension of Time Fee.

X A return postcard.

Please consider this a PETITION FOR EXTENSION OF TIME for sufficient number of months to enter these papers and please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
Customer Number 21186

By: Thomas F. Brennan
Atty: Thomas F. Brennan
Reg. No. 35,075

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Appeal Brief--Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 14TH day of January, 2005.

PETER REBUFFONI
Name

Peter Rebuf
Signature

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:		
	Alan Dowd et al.	Examiner: Dwin Craig
Serial No.:	09/483,127	Group Art Unit: 2123
Filed:	January 14, 2000	Docket: 105.176US1
For:	NETWORK SECURITY MODELING SYSTEM AND METHOD	

APPELLANTS' BRIEF ON APPEAL UNDER 37 C.F.R. 41.37(c)

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Appeal Brief is presented in support of the Notice of Appeal to the Board of Patent Appeals and Interferences, filed on June 10, 2004, from the Rejection of claims 1-42 of the above-identified application, as set forth in the Office Action mailed on June 10, 2004.

The Commissioner of Patents and Trademarks is hereby authorized to charge Deposit Account No. 19-0743 in the amount of 250.00 which represents the requisite fee set forth in 37 C.F.R. § 41.2(b)(2).

Appellants respectfully request consideration and reversal of the Examiner's rejections of pending claims 1-42.

APPELLANTS' BRIEF ON APPEAL

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest of the above-captioned patent application is the assignee, SECURE COMPUTING CORPORATION.

2. RELATED APPEALS AND INTERFERENCES

Appellants know of no other appeals or interferences which will have a bearing on the Board's decision in the present appeal.

3. STATUS OF THE CLAIMS

Claims 1-42 are pending; all of these claims have been rejected, and are the subject of the present appeal.

4. STATUS OF AMENDMENTS

All amendments have been entered. The last amendment was made in the Amendment and Response filed April 21, 2003.

5. SUMMARY OF CLAIMED SUBJECT MATTER

As noted in the Background of the present patent application, increasing amounts of information being transferred between systems internal and external to a network have made the need for improved security tools vital. Conventional network vulnerability tools do not look at the interactions of network components or show the path of an attack. These tools may not look at both the internal and external face of the network. Additionally, tools that assess vulnerabilities through controlled attacks on the network leave footprints such as log entries and may disrupt the network.

The present application describes a network securities modeling system, a method for assessing network vulnerabilities and a method for opposing network attackers. The system taught by Appellants and claimed in claims 1-17 and 34-42 includes a simulator coupled with a network configuration database and network vulnerabilities database (p. 2, lines 21-22; Fig. 1).

The network configuration database contains a plurality of network tables such as a node table, routing table, configuration table, and filter table (p. 13, line 25 – p. 14, line 1). Network configuration data may be received from an objective network, the output of a network configuration discovery tool, or a system administrator (p. 11, lines 23 – 26). Storing network configuration data allows multiple tests or attack strategies to be run on a single network configuration. Providing for user modification of the simulated network configuration data allows system administrators to either test the results of adding new components to an existing network or test the design of a non-existent network (p. 9, line 24 – p. 10, line 3). An illustration of one embodiment of the network configuration database is shown in Figure 7.

The network vulnerabilities database contains vulnerability data about conventional network components, hardware and software (p. 5, lines 10 – 12). Specifically, each entry contains the service including version and patch levels, defense conditions that might close the vulnerability, the resource and state conditions needed to exercise the vulnerability and the effects of exploiting the vulnerability (p. 17, lines 2-7).

Simulations are run to determine network vulnerabilities using vulnerability and network configuration data. The simulator is capable of simulating a variety of networks including enterprise networks, wide area networks and local area networks using the network configuration data (p. 5, lines 1-3). The simulator is also able to simulate network components such as servers, workstations, routers and firewalls, as well as the protocols and services that run on the components (p. 5, lines 3-5). The simulator analyzes interactions between network components, the interior and the exposed face of the network. Simulations can be preformed based on specific attack scenarios using configuration and vulnerability data, general attack scenarios, or attack scenarios determined by a system administrator or other user (p. 6, lines 15-17; p. 7, lines 6-9)

Appellants teach, and claim in claims 10-17, 34-37, 39 and 41-42, a mission objectives module coupled to the network simulator. The mission objectives module contains critical resource information such as goals, expectations, and constraints for simulating the network (p. 9, lines 1-3). The information may be used to determine that a particular entity is important for a specific attack scenario (p. 9, lines 3-5). Mission objectives data may be contained in a plurality of tables and modeled as components or services that need to be protected against attacks (p. 17, lines 25-32).

Appellants teach, and claim in claims 9, 38 and 39, the system implemented as an interactive computer game. The system may have a plurality of client players such as attackers, defenders, or administrators. (p. 20, lines 1-4). Clients attack the network by sending commands that simulate service functionality, change services or nodes, and exploit vulnerabilities (p. 20, lines 14-15). Clients defend network territory by adjusting the posture of nodes, setting router and firewall filtering policies, and resetting nodes or services that have been disabled or compromised (p. 20, lines 15-17). The system may be used either for entertainment or as a training tool to educate personnel involved with network security in building and protecting secure networks (p. 20, lines 5-7).

Appellants teach, and claim in claims 18-27, a method of analyzing computer network security using a modeling system. As shown at p. 2, lines 25-30, Figure 1and p. 4, line 28 through p. 7, line 26, the method comprises providing a network configuration of a computer network, simulating the network based on the configuration, and determining vulnerabilities of the simulated network using the vulnerability information stored in the database.

Appellants teach, and claim in claims 28-33, a method of opposing network attackers. As shown at p. 3, lines 1-6, Figure 3 and p. 11, line 6-22, the method includes receiving a network configuration, receiving mission objectives, receiving commands from a network attacker, simulating the network based on the commands received from the attacker, and responding to the network attacker.

6. ISSUES PRESENTED FOR REVIEW

Are claims 1-8 and 18-27 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and in further view Samfat?

Are claims 9, 38 and 39 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and in further view of Samfat, Sparks II (U.S. Patent No. 6,352,479), and Jackson?

Are claims 10-17 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Ptacek (U.S. Patent No. 6,343,362), and in further view of Samfat, Bergman (U.S. Patent No. 6,442,694), and Smith Jr. (U.S. Patent No. 5,662,478)?

Are claims 28-33 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Gleichauf (U.S. Patent No. 6,324,656), in view of Johnson, and in further view of Samfat, Kurtzberg (U.S. Patent No. 5,961,644), and Jackson?

Are claims 34-37 and 40-42 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Johnson, in view of Porras (U.S. Patent No. 6,321,338), and in further view of Gleichauf (U.S. Patent No. 6,282,546)?

7. ARGUMENT

Rejections under U.S.C. § 103

1) The Applicable Law

According to *M.P.E.P.* § 2141, which cites *Hodosh v. Block Drug Co., Inc.*, 786 F.2d 1136, 1143 n.5, 229 USPQ 182, 187 n.5 (Fed. Cir. 1986), the following tenets of patent law must be adhered to when applying 35 U.S.C. § 103. First, the claimed invention must be considered as a whole. Second, the references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination. Third, the references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention. Fourth, obviousness is determined using a reasonable expectation of success standard. Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. *M.P.E.P.* § 2141 (citing *Graham v. John Deere*, 383 U.S. 1, 148 USPQ 459 (1966)).

The Examiner has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *M.P.E.P.* § 2142 (citing *In re Vaeck*, 947 F.2d, 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on Appellants' disclosure. *M.P.E.P.* § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). The references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references.

M.P.E.P. § 2142 (citing *Ex parte Clapp*, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985)). In considering the disclosure of a reference, it is proper to take into account not only specific teachings of the reference but also the inferences which one skilled in the art would reasonably be expected to draw therefrom. *M.P.E.P.* § 2144.01 (citing *In re Preda*, 401 F.2d 825, 826, 159 USPQ 342, 344 (CCPA 1968)). However, if the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *M.P.E.P.* § 2143.01 (citing *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984)).

In order to take into account the inferences which one skilled in the art would reasonably make, the examiner must ascertain what would have been obvious to one of ordinary skill in the art at the time the invention was made, and not to the inventor, a judge, a layman, those skilled in remote arts, or to geniuses in the art at hand. *M.P.E.P.* § 2141.03 (citing *Environmental Designs, Ltd. v. Union Oil Co*, 713 F.2d 693, 218 USPQ 865 (Fed. Cir. 1983), *cert. denied*, 464 U.S. 1043 (1984)).

> The examiner must step backward in time and into the shoes worn by the hypothetical "person of ordinary skill in the art" when the invention was unknown and just before it was made. In view of all factual information, the examiner must then make a determination whether the claimed invention "as a whole" would have been obvious at that time to that person. Knowledge of Appellants' disclosure must be put aside in reaching this determination, yet kept in mind in order to determine the "differences," conduct the search and evaluate the "subject matter as a whole" of the invention. The tendency to resort to "hindsight" based upon Appellants' disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.

M.P.E.P. § 2141.03.

2) *Application of §103 Law to the Rejected Claims*

Claims 1-8 and 18-27 were rejected under 35 USC § 103(a) as being unpatentable over Gleichauf in view of Ptacek and in further view of Samfat.

Gleichauf describes a system and method for characterizing a network and identifying vulnerabilities. As noted by the Examiner, Gleichauf discloses a network configuration module having network configuration data. In contrast to Appellants, however, Gleichauf identifies and tests vulnerabilities by applying a rule set (col. 4, lines 43-47, col. 7, lines 6-31 and Fig. 4) to identify vulnerabilities and then testing the actual network to see if the vulnerabilities exist.

Appellants teach that it can be difficult to test vulnerabilities on the network itself. As noted on p. 1, lines 28-30, such tests can disrupt the network and may leave footprints such as event log entries and the like on scanned machines. Therefore, in contrast to Gleichauf, Appellants teach the use of a separate simulator to identify and test vulnerabilities.

The Examiner stated that Gleichauf discloses a security modeling system having a network configuration module and a network vulnerabilities database but that Gleichauf does not disclose a network simulation for analyzing attacks against a network. The Examiner stated that Ptacek "discloses a network simulation for analyzing attacks against a network." Appellants disagree.

Ptacek describes a higher-level computer language that can be used to create programs that simulate attacks against a computer network. Ptacek describes how the language is used to generate network traffic to test an existing network for known vulnerabilities. Ptacek does not, therefore, describe a network simulation for analyzing attacks against a network, but instead describes a computer language for generating attacks against the network itself. Appellants respectfully request that this rejection be withdrawn.

The Examiner stated that Gleichauf does not disclose a network simulation. The Examiner stated that Samfat "discloses a network simulation."

Samfat describes a mobile network simulator used to test software applications, specifically a generic intrusion architecture. The network modeled in Samfat is composed of three parts, a Mobile Station (MS), Base Station Sub-system (BSS) and Network Switching Sub-system (NSS). While the system is scalable, it is customizable only in respect to the number of each component in a given topology. For example, there may be a varying number of MS's, but each MS communicates only with a BSS through an air interface. Similarly, there may be a varying number of BSS's, but each BSS communicates only with a number of MS's and a single MSC, as shown in figures 1 and 2, and discussed at p. 766 and 767. The network simulation described in Samfat is limited to a narrow field of mobile networks. In contrast, Appellants describe a network simulator that simulates enterprise networks, wide area networks, local area networks and the like as well as components of networks such as servers, workstations, routers and firewalls (p. 5, lines 2-5). Therefore, while Samfat discloses a network simulation, the simulator described by Appellants is of a substantially different character.

The Examiner stated that it would have been obvious to combine Gleichauf with Samfat because, "by being able to exactly repeat the manner in which the network behaves as the attack takes place, software counter measures can be tested, and then retested in an environment where the same conditions can be repeated when debugging the counter measure software," (Office Action, p. 9). Samfat teaches that by using a simulator to develop a Network Management System problems unique to a mobile network are avoided. Specifically, problems involving the unavailability of existing networks during the software development phase and the provision of a wide range of traffic generators over a wide geographic area are avoided. Samfat also teaches that simulators allow repeatability over excessive runs and the value of a static network configuration for repeatable software testing. In contrast, Appellants teach a system for assessing network vulnerabilities in an objective network, and not for debugging software. This is significant, because while in some cases similar conditions may be repeated, Appellants teach that by allowing the system administrator or user to modify configuration data, information can be gleamed as to what effect adding or removing a device might have on the objective network before physically modifying the network (p. 6, lines 12-17). Because the simulators are significantly different themselves and also because the purpose and use of the simulators are distinct, it would not have been obvious to combine the references. Appellants respectfully request that this rejection be withdrawn.

Even if the references are combined, the combination does not teach the claimed invention. Gleichhauf teaches a method comprising a host discovery phase, a data collection phase, an analysis phase and an active analysis phase for confirming the potential vulnerabilities identified. Gleichauf does not disclose general attacks against the network, instead limiting the active analysis phase to verifying the existence of vulnerabilities determined by acting upon the configuration database with a rule set (Col. 8, lines 13-18). In comparison, Appellants teach that the simulator can be used for both specific attack scenarios or general attack scenarios (p. 6, lines 15-17). In addition, user defined security checks are disclosed by Appellants (p. 7, lines 7-9). Therefore, no combination of the references disclose the more rigorous simulation and analysis described by Appellants.

The Examiner stated that Gleichauf discloses

> a computer implemented method of analyzing networks based on the network configuration data where the software includes a network vulnerabilities database where the network vulnerabilities database includes, a plurality of known network vulnerabilities where each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

Office Action p. 8. The system described by Gleichauf creates a network vulnerabilities database using rules applied to information in the port database. Gleichauf teaches using three rules; the first to determine an operating system, the second to determine a service and the third to determine a potential vulnerability. Thus, while Gleichauf describes a database of network vulnerabilities organized in a hierarchical structure where each entry contains an operating system represented by the entry, a service to which it applies and a potential vulnerability, the reference does not teach that these vulnerabilities include "defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability," (Claims 1 and 18).

Appellants respectfully request that the Examiner's rejection of claims 1-8 and 18-27 be reversed.

Claims 9, 38 and 39 were rejected under 35 USC § 103(a) as being unpatentable over Gleichauf in view of Ptacek and in further view of Samfat, Sparks and Jackson.

Gleichauf, Ptacek, and Samfat are discussed above. As noted above none of the references teach a simulator similar to that claimed by Appellants. Also, the combination of the references is non-obvious, as previously discussed.

The Examiner stated that Gleichauf did not disclose a computer game. The Examiner stated that Jackson discloses a game, and Sparks discloses a computer game.

Jackson describes a card game based on the Illuminati system. The card game uses hacker terminology to create a game in which players try to gain access to one or more cards representing computer systems. The game described by Jackson builds a network during game play by laying cards down in a domino-like manner. However, the use of hacker and network terminology in the game is a superficial change of a pre-existing card game (compare Jackson to Jackson2). In contrast, Appellants teach a game with a modeled network that behaves accurately enough to train system administrators and other personnel on how to build and protect secure networks (p. 20, lines 5-7). The Examiner stated that combining Gleichauf with Jackson would have been obvious because Jackson shows "modeling a computer network and pretending to hack into that network are activities that people like to do," (Office Action p. 32). While Jackson does teach that playing an Illuminati style card game is something people like to do, the reference does not show that playing a computer game involving attacking or defending an accurate simulation of a realistic network is something people like to do.

Sparks describes a system for screening players in an online multiplayer game system. Sparks teaches that by screening players, the players are more likely to compete against opponents of equal skill level with preferences agreeable to most of the players involved. Even if Sparks describes an attacker and a defender in the context of an Internet-based game, there is no teaching or motivation in any of the cited references to create an environment where an attacker can attack a computer network through a simulation of that network and a defender defend that same simulated network.

Appellants respectfully submit that the Office Action relied on the Appellants' disclosure and/or impermissible hindsight in forming the rejection of claim 9 over the cited references. As such, Appellants respectfully request that the Examiner's rejection of claims 9, 38 and 39 be reversed.

Claims 10-17 were rejected under 35 USC § 103(a) as being unpatentable over Gleichauf in view of Ptacek and in further view of Samfat, Bergman, and Smith Jr.

Gleichauf, Ptacek, and Samfat are discussed above. As noted above none of the references teach a simulator similar to that claimed by Appellants. Also, the combination of the references is non-obvious.

The Examiner stated that Gleichauf does not disclose a mission objectives module coupled to the simulator used to determine network components that are involved in a specific attack scenario. The Examiner stated that Bergmann discloses determining network components that are involved in a specific attack scenario.

Bergmann describes a method and a system for isolating faults in high speed communications networks. Bergmann teaches that the inability to determine if a fault is caused by an attack or failure coupled with the inability to determine the source of an attack can result in unnecessary shutdowns and delays. While Bergmann has relevance in network security applications, the system does not serve the purpose that the Appellants' mission objective module does in determining components involved in an attack scenario. Appellants teach knowing which components are likely to be involved in an attack scenario before and after the simulation is run in order to assess the security of the network. In contrast, Bergmann teaches a defensive method and system for protecting the integrity and efficiency of a network against an attack in progress.

The Examiner stated that Smith Jr. discloses mission objectives. Smith Jr. describes a tool useful in creative thinking sessions. Regardless of whether Smith Jr. teaches mission objectives, or missions and objectives, they are of a distinctly different character than the mission objectives module Appellants disclose. Missions and objectives in the context of Smith Jr. relate to generic problem solving goals. In contrast, Appellants teach mission objectives of a different kind, used to determine which components are involved in a specific network simulation and including critical resource information.

No combination of the references teaches a mission objectives module coupled to the simulator used to determine network components that are involved in a specific attack scenario. Appellants respectfully request that the Examiner's rejection of claims 10-17 be reversed.

Claims 28-33 were rejected under 35 USC § 103(a) as being unpatentable over Gleichauf in view of Johnson and in further view of Samfat, Kurtzberg, and Jackson.

Gleichauf and Samfat are discussed above. As noted above none of the references teach a simulator similar to that claimed by Appellants. Also, the combination of the references is non-obvious.

The Examiner stated that Jackson discloses mission objectives. Jackson describes mission objectives in the context of gaining access to a given number of systems in order for a player to win a game. In contrast, Appellants teach using mission objectives that include critical resource information in order to determine components involved in a specific attack scenario. Also, as discussed above, there is no motivation to combine the references, because Jackson does not teach an accurate model of a network, but rather a stylized card game using hacker terminology.

No combination of the references teaches receiving mission objectives including critical resource information used to determine network components that are involved in a specific attack scenario. Appellants respectfully request that the Examiner's rejection of claims 28-33 be reversed.

Claims 34-37 and 40-42 were rejected under 35 USC § 103(a) as being unpatentable over Johnson in view of Porras and in further view of Samfat and Gleichauf 2.

Samfat is discussed above. As noted above, the reference does not teach a simulator similar to that claimed by Appellants.

The Examiner stated that Johnson "discloses a security modeling system for simulating networks and to determine network components that are involved in a specific attack scenario including configuration data," (Office Action, p. 28). Appellants disagree. Johnson discloses a security system that launches attacks against an existing network in order to determine possible vulnerabilities. Johnson also teaches obtaining information such as which network components are involved in a specific attack and configuration data through a controlled attack on an existing network. However, Johnson does not teach a security modeling system for simulating networks.

The Examiner stated that Gleichauf 2 discloses a plurality of data bases including mission objective tables, vulnerability tables and network configuration tables. Gleichauf 2 describes a system and method for inserting data into a multi-dimensional database in real time. Gleichauf 2 discusses the application of this system to network intrusion detection and vulnerability assessment systems. While Gleichauf 2 does disclose vulnerability tables and network configuration tables, the reference does not disclose mission objective tables. Appellants teach that mission objective tables are a valuable tool in determining attack scenarios and also for evaluating network security.

Appellants respectfully request that the Examiner's rejection of claims 34-37 and 40-42 be reversed.

It is respectfully submitted that the cited art neither anticipates or renders the claimed invention obvious and that therefore the claimed invention does patentably distinguish over the cited art. It is respectfully submitted that claims 1-42 should therefore be allowed. Reversal of the Examiner's rejections of claims 1-42 is respectfully requested.

Respectfully submitted,

ALAN DOWD et al.

By their Representatives,

SCHWEGMAN, LUNDBERG,
WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402

Date January 14, 2005 By Thomas F. Brennan
Thomas F. Brennan
Reg. No. 35,075

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 14 day of January, 2005.

Peter Rebuffoni
Name

Peter
Signature

APPENDIX I

The Claims on Appeal

1. (Previously Presented) A security modeling system comprising:

a network configuration module having network configuration data;

a simulator coupled to the network configuration module to simulate and analyze networks based on the network configuration data, wherein the simulator includes a network vulnerabilities database, and wherein the network vulnerabilities database includes:

a plurality of known network vulnerabilities, wherein each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

2. (Original) The system of claim 1, wherein the network vulnerabilities database includes network vulnerability, attack and exploitation data.

3. (Original) The system of claim 2, wherein the network configuration data and the network vulnerability, attack and exploitation data are stored in database tables and the data is processable by a computer.

4. (Original) The system of claim 1, wherein the network configuration module comprises network configuration data output by a network configuration discovery tool.

5. (Original) The system of claim 1, wherein the simulator includes a graphical user interface.

6. (Original) The system of claim 2, wherein the simulator includes a means for receiving the network vulnerability, attack and exploitation data.

7. (Original) The system of claim 1, wherein the simulator includes a defender and an attacker user interface.

8. (Original) The system of claim 1, wherein the security modeling system is portable.

9. (Original) A computer game comprising:

a network configuration module having network configuration data;

a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration, wherein the simulator includes a network vulnerabilities database, and wherein the simulator includes a graphical user interface for playing the game.

10. (Previously Presented) A security modeling system comprising:

a network configuration module having network configuration data;

a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration, wherein the simulator includes a network vulnerabilities database; and

a mission objectives module coupled to the simulator, wherein the mission objectives module includes critical resource information used to determine network components that are involved in a specific attack scenario.

11. (Original) The system of claim 10, wherein the network vulnerabilities database includes network vulnerability, attack and exploitation data.

12. (Original) The system of claim 11, wherein the network configuration data and the network vulnerability, attack and exploitation data is stored in database tables and the data is processable by a computer.

13. (Original) The system of claim 10, wherein the simulator includes a graphical user interface.

14. (Original) The system of claim 10, wherein the critical resource information includes goals, expectations and constraints for simulating the network.

15. (Original) The system of claim 10, wherein the simulator includes a means for receiving the network vulnerability, attack and exploitation data.

16. (Original) The system of claim 10, wherein the security modeling system is portable.

17. (Original) The system of claim 10, wherein the simulator includes a defender and an attacker interface.

18. (Previously Presented) A method of analyzing a computer network using a security modeling system, wherein the security modeling system includes a database of network vulnerability information, the method comprising:

providing a network configuration of a computer network;

simulating the network based on the network configuration; and

determining vulnerabilities of the simulated network using the vulnerability information stored in the database, wherein the database includes a plurality of known network vulnerabilities, wherein each network vulnerability includes:

> a plurality of known network vulnerabilities, wherein each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

19. (Original) The method of claim 18, wherein providing a network configuration includes receiving a configuration as the output of a network discovery tool.

20. (Original) The method of claim 18, wherein providing a network configuration includes receiving a data file which includes a configuration of the computer network.

21. (Original) The method of claim 18, wherein simulating the network includes:

receiving mission objectives;

storing the objectives; and

simulating the network based on the network configuration and mission objectives.

22. (Original) The method of claim 21, wherein determining vulnerabilities includes modifying the simulation using a graphical user interface.

23. (Original) The method of claim 22, wherein modifying the simulation includes dynamically interacting with an attacker.

24. (Original) The method of claim 22, wherein modifying the simulation includes dynamically interacting in real time with the security modeling system.

25. (Original) The method of claim 23, wherein modifying the simulation includes dynamically interacting in real time with the security modeling system.

26. (Original) The method of claim 21, wherein determining vulnerabilities includes computing security results, wherein the security results include a security score.

27. (Original) The method of claim 21, wherein determining vulnerabilities of the simulated network includes updating the vulnerabilities database when vulnerabilities are detected.

28. (Previously Presented) A method of opposing network attackers comprising:

receiving a network configuration, wherein the network configuration comprises computer hardware and software component information;

receiving mission objectives including critical resource information used to determine network components that are involved in a specific attack scenario;

receiving commands from a network attacker;

simulating the network based on the commands received from the network attacker, wherein simulating the network includes determining results as a function of the network configuration, mission objectives and stored vulnerability data for the described computer hardware and software components; and

responding to the network attacker, wherein responding to the attacker includes imposing barriers, providing response messages and protecting the network.

29. (Original) The method of claim 28, wherein simulating the network further includes receiving commands from a defender and determining results based on the defender commands.

30. (Original) The method of claim 28, wherein receiving configuration includes receiving critical resource information, wherein the critical resource information includes goals, expectation and constraints for simulating the network.

31. (Original) The method of claim 28, and further includes modifying the simulation using a graphical user interface.

32. (Original) The method of claim 31, wherein determining vulnerabilities includes computing security results which include a security score.

33. (Original) The method of claim 31, wherein receiving commands includes receiving attack actions which include commands that simulate service functionality, commands that change services or nodes, and commands that exploit vulnerabilities.

34. (Previously Presented) A security modeling system for simulating objective networks comprising:

a simulator having a plurality of databases, wherein the plurality of databases include mission objectives tables including information used to determine network components that are involved in a specific attack scenario, vulnerability tables, and network configuration tables, wherein the network configuration tables include network configuration data; and

a graphical user interface which operates with the simulator to allow input and output to clients.

35. (Original) The system of claim 34, wherein the mission objectives tables include mission tables, mission files tables and mission services tables.

36. (Original) The system of claim 34, wherein the vulnerability tables include service tables.

37. (Original) The system of claim 34, wherein the network configuration tables include configuration tables, defense tables, filter tables, node tables, routing tables and password tables.

38. (Previously Presented) The computer game of claim 9, wherein the simulator further comprises:

an attacker interface to transmit real-time network status information to an attacker during a simulation; and

a defender interface to transmit real-time network status information to a defender during a simulation.

39. (Previously Presented) The computer game of claim 9 further comprising:

a mission objectives module coupled to the simulator, wherein the mission objectives module includes critical resource information used to determine network components that are involved in a specific attack scenario.

40. (Previously Presented) A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

providing a network configuration of a computer network;

simulating the network based on the network configuration; and

determining vulnerabilities of the simulated network using the vulnerability information stored in the database, wherein the database includes:

a plurality of known network vulnerabilities, wherein each network vulnerability includes the service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

41. (Previously Presented) The machine-readable medium of claim 40, wherein simulating the network includes:

receiving mission objectives;

storing the objectives; and

simulating the network based on the network configuration and mission objectives.

42. (Previously Presented) The machine-readable medium of claim 41, wherein mission objectives include critical resource information used to determine network components that are involved in a specific attack scenario.